# REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188



| 1. AGENCY USE ONLY ( Leave Blank) | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | 3 March 2003 | Final 9 April 2002 – 8 January 2003 |

4. TITLE AND SUBTITLE

Noisy Quantum Computation and Communication

5. FUNDING NUMBERS

DAAD19-02-1-0065

6. AUTHOR(S)

Mary Beth Ruskai

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

UMass Lowell, 600 Suffolk St., Lowell, MA 01854

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

43509.1-PH-QC

11. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

When quantum particles are used to transmit information, one can expect that, as with classical communication, noise in the channel will affect the fidelity of the transmission. This is true whether the particles are used to transmit quantum or classical information. Similar concerns arise in quantum computation when the noise due to interactions with the environment gives rise to errors. This project has been concerned with the analysis of noise that breaks entanglement and with the development of new codes for quantum error correction.

14. SUBJECT TERMS

quantum information theory, channel capacity, error correction

15. NUMBER OF PAGES
8

16. PRICE CODE

| 17. SECURITY CLASSIFICATION OR REPORT | 18. SECURITY CLASSIFICATION ON THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | UL |

NSN 7540-01-280-5500

Standard Form 298 (Rev.2-89)
Prescribed by ANSI Std. 239-18
298-102

Report Documentation Page (SF298 Continuation)

# Final Project Report

# Noisy Quantum Computation and Communication

## Contents



## A Overview

When quantum particles are used to transmit information, one can expect that, as with classical communication, noise in the channel will affect the fidelity of the transmission. This is true whether the particles are used to transmit quantum or classical information. Similar concerns arise in quantum computation when the noise due to interactions with the environment gives rise to errors.

This project has been concerned with the analysis of mathematical models of noise and with the development of new codes for quantum error correction. Because of the P.I.'s move from Lowell to Tufts, this report on covers only the 8-month period. April-December, 2002. The first three months overlapped with an earlier ARO grant and results obtained in that time were also included in the final report for DAAG55-98-1-0374.

# B Summary of Results

## B.1 Entanglement Breaking channels

Recently, there has been interest in channels which break entanglement in the sense that action on one part of an entangled state always results in a separable one. These channels can also be simulated by classical channels and can be written in the form

$$\Phi(\rho) = \sum_k R_k \operatorname{Tr} F_k \rho \tag{1}$$

where each $R_k$ is a density matrix and the $\{F_k\}$ form a POVM. Holevo [5] introduced this form and two subclasses; a channel is called

- *classical-quantum* (CQ) if each $F_k = |k\rangle\langle k|$ in the POVM is a one-dimensional projection,
- *quantum-classical* (QC) if $\sum_k R_k = I$ and each density matrix $R_k = |k\rangle\langle k|$ is a one-dimensional projection.

Mathematically, a channel is a completely positive trace-preserving map (CPT); those which break entanglement will be denoted as EBT.

Holevo [4] gave examples of particular CQ maps for which entangled measurements can increase the capacity of the channel. However Shor [17] showed that entangled inputs cannot further increase the capacity of such channels. In related developments, Vidal, Dür and Cirac [18] used Shor's techniques to find the entanglement cost for a class of mixed states associated with EBT maps; and Matsumoto, Shimono and Winter [9] showed a connection between additivity of channel capacity and entanglement of formation. Quite recently, King [7] showed that the measures of purity known as maximal p-norms, as well as minimal entropy, are multiplicative for EBT maps.

Because it is important to understand the distinction between channels which break entanglement, those which preserve certain types of entanglement, and those which may be enhanced by entanglement (in the sense that entangled inputs can increase capacity), the P.I. undertook a more detailed study of EBT maps.

In [15], the P.I. gave a rather complete analysis of EBT maps in the case of qubits, and presented some basic results for channels in $d$-dimensions. One of the main result for qubits is that the set of EBT maps is precisely the convex hull of CQ channels. Subsequently, Shor found an example of a map for $d = 3$ which is an extreme point of the set of EBT maps, but is not CQ. Shortly after this, in November, 2003, M. Horodeck, P. Shor and the P.I. met during a workshop at MSRI and obtained a number of additional results about the extreme points of general EBT maps. These results are described in [6].

It was shown that the set of EBT maps is convex and that the following are equivalent ways of characterizing them.

(A) $\Phi$ can be written in the form (1).

(B) $\Phi$ is entanglement breaking, i.e., $(I \otimes \Phi)(\Gamma)$ is separable for any input density matrix $\Gamma$.

(C) $(I \otimes \Phi)(|\beta\rangle\langle\beta|)$ is separable when $|\beta\rangle$ is maximally entangled.

(D) $\Phi$ can be written in operator sum form using only Kraus operators of rank one.

(E) $\Upsilon \circ \Phi$ (or, equivalently, $\Phi \circ \Upsilon$) is completely positive for all positivity preserving maps $\Upsilon$.

A number of additional results about extreme points of the set of EBT maps, the action of $I \otimes \Phi$ on a maximally entangled states, and the structure of the Kraus operators are given in [6].

In the case of qubits, it suffices to let $\Upsilon$ be the transpose, because the positive partial transpose (PPT) condition is then sufficient for distinguishing between separable and entangled states. This immediately gives rise to other results, such as equivalence with a "sign change" condition in a canonical parameterization [8, 14]. These results are contained in [16].

## B.2 Quantum Error Correction

Quantum error correction is now well-developed in the case of so-called stabilizer codes, which arise as invariant subspaces of Abelian subgroups of the Pauli group. These codes generalize some classical ideas, such as Hamming distance, to quantum settings and seem best suited to situations in which all one-bit errors are equally likely and the noise is uncorrelated. Unfortunately, their use in full-scale fault tolerant computation involves concatenations requiring a large number of physical qubits for each logical unit.

In realistic models of quantum computers, it may be possible to protect against some types of one-bit errors so that, e.g., phase errors are less (or more) likely than bit flips. On the other hand, at least some types of correlated errors will be more probable than arbitrary two-bit errors (and possibly than certain one-bit errors). Therefore, one is interested in more general types of code construction which can be adapted to deal with the most probable errors. It is known [1, 11, 12] that other types of quantum codes, often called "non-additive," exist, but they have not been studied extensively.

Together with H. Pollatsek, the P.I. began to study the natural generalization of stabilizer codes to codes associated with the action of non-Abelian groups. We are

particularly interested in the use of higher dimensional representations for the correction of two-bit errors, and the ways in which the degeneracy allows the correction of more two-bit errors than would be expected by dimensional arguments alone.

Thus far, we have considered the special case of permutationally invariant codes, which can be regarded as stabilizers of the symmetric group. We found a number of new codes. In particular, we found two new 7-bit codes which are impervious to exchange and can correct all 1-bit errors. We have also studied the types of two-bit errors they can correct; although unlikely to be of practical use, we established that degeneracy enhancement for two-bit errors does occur. Using this perspective, we showed that the classical 5-bit repetition code can also correct more two-bit quantum errors than those associated with a single type of one bit error.

We also found a large family of new permutationally invariant 9-bit codes in addition to the simple one found by the P.I. [13] earlier. Such codes would be particularly useful if the additional two bits could be used to correct one class of double errors of the same type, e.g., all pairs of bit flips, in addition to all 1-bit errors. Although the structure of the irreducible representations suggests that this might be possible, analysis of the required conditions shows that they do not have a solution. We need to better understand the implications of this, as well as those combinations of single and double bit errors that can be corrected.

Constructing permutationally invariant codes was not intended as an end in itself, but as a first step in the development of a theory of non-Abelian stabilizer codes. (Indeed, permutationally invariant codes would be ill-suited for quantum computers which use exchange interactions to implements gates.) From this perspective, the results obtained are quite interesting, and indicate that stabilizer codes associated with other groups merit investigation. A paper containing our results on permutationally invariant codes has been written and should be available soon.

# C List of Publications

a) "Entanglement Breaking Channels" posted at arXiv.org/abs/quant-ph/0201700, but now superseded by (b) and (c).

b) "Entanglement Breaking Channels" submitted to *Rev. Math. Phys.* and posted at arXiv.org/abs/quant-ph/0302031 [with M. Horodeck and P. Shor] includes a significant revision of section 3 of (a), as well as new results.]

c) "Qubit Entanglement Breaking Channels" submitted to *Rev. Math. Phys.* and posted at arXiv.org/abs/quant-ph/0302032 includes of section 2 of (a).

d) "Permutationally Invariant Codes for Quantum Error Correction" in preparation [with H. Pollatsek].

# D Scientific personnel and student training

The P.I. has continued to help advise Michael Nathanson, a student of Chris King at Northeastern University, who was supported by the previous ARO grant in summer, 2001. Nathanson [10] recently obtained a quantum algorithm for a "Guessing Secrets" problem motivated by a practical problem in internet routing. His results improve the complexity of the critical guessing phase from $O(\log N)^3$ to $O(1)$ and the overall complexity from $O(\log N)^3$ to $O(\log N)$. His work may be the first in which a variant of the Deutsch-Jozsa algorithm is used to solve a practical problem, rather than an artificial one designed to illustrate theoretical complexity. The P.I.'s role has been primarily to encourage Nathanson to explore the complexity issues and their implications for the development of quantum algorithms for new classes of problems.

In the summer of 2002, John Cortese, a graduate student with John Preskill at Caltech, spent 8 weeks working with the P.I.; some travel and subsistence for his visit were provided by this grant. Most of his time was spent on numerical studies of capacity questions. Although these turned out to be too delicate numerically to resolve in the time of his visit (or with the software available), considerable progress was made in identifying those types of qubit channels which require three or four non-orthogonal inputs to maximize channel capacity. This is an important step in understanding when entangled inputs might enhance capacity; a question which has since been shown [9] to also be relevant to the computation of entanglement cost and the entanglement of formation.

Matt Noonan, a student at Hampshire College, is doing his senior thesis on a question of entanglement classification. The P.I. has observed that evenly weighted superpositions of all possible product states in the so-called computational basis form an interesting subclass of states, which can be endowed with a simple group structure corresponding to pointwise addition. The product states (in a basis rotated by the Hadamard transform) form a subgroup with respect to which one expects all members of a given coset to have the same entanglement. These cosets typically contain highly entangled states, such as GHZ states and some of Briegel's [2, 3] so-called "cluster states". Thus, it is natural to ask if this group structure gives rise to a small set of parameters which can be used to characterize highly entangled states. In view of the large numbers of invariants associated with multi-particle entanglement and the difficulty of finding a complete classification system, this could be quite useful. Thus far, Nathanson has succeeded in recovering the expected results for bipartite entanglement.

# References


[1] V. Arvind, "Nonstabilizer quantum codes from Abelian subgroups of the error group" quant-ph/0210097.

[2] H. J. Briegel, R. Raussendorf, "Persistent entanglement in arrays of interacting particles" quant-ph/0004051.

[3] R. Raussendorf, D.E. Browne and H. J. Briegel, "Measurement-based quantum computation with cluster states" quant-ph/0301052

[4] A. S. Holevo, "The capacity of quantum channel with general signal states", *IEEE Trans. Info. Theory* preprint available at xxx.lanl.gov/abs/quant-ph/9611023

[5] A. S. Holevo, "Coding Theorem for Quantum Channels" quant-ph/9809023; "Quantum coding theorems", *Russian Math. Surveys*, vol. 53:6, pp. 1295-1331, 1999.

[6] M. Horodecki, P. Shor and M.B. Ruskai "Entanglement Breaking Channels submitted to *Rev. Math. Phys.* and posted as quant-ph/0302031

[7] C. King, "Maximal p-norms of entanglement breaking channels" quant-ph/0212057

[8] C. King and M.B. Ruskai "Minimal Entropy of States Emerging from Noisy Quantum Channels" *IEEE Trans. Info. Theory* **47**, 1–19 (2001). quant-ph/9911079

[9] K. Matsumoto, T. Shimono and A. Winter, "Remarks on additivity of the Holevo channel capacity and of the entanglement of formation" quant-ph/0206148

[10] M. Nathanson, "Quantum Guessing via Deutsch-Jozsa" quant-ph/0301025

[11] E.M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane "A nonadditive quantum code" *Phys.Rev.Lett.* **79**, 953–954 (1997). (quant-ph/9703002)

[12] V. P. Roychowdhury and F. Vatan, "On the Structure of Additive Quantum Codes and the Existence of Nonadditive Codes" quant-ph/9710031

[13] M.B. Ruskai, "Pauli Exchange Errors in Quantum Computation" *Phys. Rev. Lett* **85**, 194-197 (2000). quant-ph/9906114

[14] M.B. Ruskai, S. Szarek and E. Werner, "An analysis of completely positive trace-preserving maps on $\mathcal{M}_2$" *Lin. Alg. Appl.*. **347**, 159–187 (2002).

[15] M.B. Ruskai, "Entanglement Breaking Channels posted at arXiv.org/abs/quant-ph//0201700. Superseded by [6, 16].

[16] M.B. Ruskai, "Qubit Entanglement Breaking Channels submitted to *Rev. Math. Phys.* and posted as quant-ph/0302032

[17] P. Shor, "Additivity of the Classical Capacity of Entanglement-Breaking Quantum Channels" *J. Math. Phys.* **43,** 4334-4340 (2002).

[18] G. Vidal, W. Dür, J.I. Cirac, "Entanglement cost of mixed states" quant-ph/0112131